A Case Study Examining Trends in Company Information Security Attacks and Their Implication for the Future of Computer Science

Mohammad Rafi* & Ahmad Hasan**

*Researcher, Department of Computer Scinece, Payame Noor University, Iran. E-Mail: rafi.mohammad27@gmail.com
**Professor, Department of Computer Science, Payame Noor University, Iran. E-Mail: ahmad.hasen22@yahoo.com

Received : 24.02.2019 **Revised : 19.05.2019** **Accepted : 24.07.2019**

***Abstract*---** From the analysis in this study, internal attacks form the major source of threat in many companies. Specifically, the analysis establishes that rogue employees accessing the administrators' accounts, sensitive data, or networks could cause real damage, rated at the medium risk rating and priority rating, with the impact and likelihood of occurrence standing at 3. Regarding the compromise of corporate services, it is established that the damage is likely to stretch beyond the loss of the ability to run daily functions within the stock inventory-systems and the online store. With the risk rating and priority rating suggesting that this destabilization of corporate services at VG Trading Company could yield medium-level damage, additional adversities. For example, a compromise to VG Trading Company's corporate services is projected to yield substantial financial losses accruing due to the loss of corporate data and the loss of contract or business. Financial loss is also projected to face VG Trading Company due to disrupted trading (such as stalled progress in online transactions), loss of money, and a loss of financial data; such as payment card details and bank details. Indeed, the latter adversities are not only likely to arise due to compromised corporate services but also as a result of unauthorized access and even data misuse by authorized employees, especially those who access company sensitive information and exhibit malicious intentions.

***Keywords*---** Security, Network, Financial Data

I. INTRODUCTION

FROM the previous scholarly investigations, costs are also projected to be incurred by VG Trading Company towards repairing the affected devices, networks, and systems, should the aforementioned cyber security threats be implemented while targeting the respective systems and company functions. Apart from the financial loss, another risk that VG Trading Company faces entails reputational damage. According to Walker and Conway (2015), trust forms an essential element steering company customer relationships. Therefore, the selected company's cyber attacks accruing from the misuse of sensitive information by sections of its employees could damage the reputation of the organization and even erode the trust of current and future customers. From this risk of reputational damage, specific adversities are predicted to include reduction in profits, loss of sales, and loss of customers. Similarly, the risk of reputational damage arising from the leakage of customer information is likely to stretch beyond the affected customer bases to impact on suppliers, compromising the company's relationship with investors and partners, as well as third parties vested in VG Trading Company. Additionally, VG Trading Company's stock-inventory systems and the online store exhibit a medium risk of cyber insecurity in terms of denial of service, which could yield additional losses of sales due to the failure by customers and suppliers to access its online store. In addition, a denial service due to the vulnerable nature of interactions between the company's IT staff and external vendors could lead to less revenue in the long-term, should most of the customers decide against doing business with the company (due to its vulnerability to attacks that yield a denial of service).

II. INFORMATION SECURITY IMPACT ANALYSIS

Should cyber insecurity events occur at VG Trading Company, it is projected that hidden costs are likely to amount to about 90 percent of the organization's total business impact but these results are likely to emerge about two or more years after the occurrence. Well-known and surface cyber incident costs are expected to include technical investigations, cyber security improvement costs, attorney fees and litigation, crises or public relations communications, regulatory compliance or fines, post-breach customer protection, and customer breach notifications. On the other

10.9756/SIJCSEA/V7I4/03010020403
ISSN: 2321-2381

hand, an occurrence of a cyber security event at VG Trading Company is likely to prompt less visible, hidden, or below the surface costs such as the loss of intellectual property, devaluation of the trade name, costs related to the value of lost contract revenue, lost value of customer relationships, operational disruption, increased cost to raise debt, and insurance premium increases. Imperative to highlight is that operational disruption forms a major business impact that the threats are likely to cause, translating into economic costs. The following table indicates specific costs of impacts, should a breach such as a loss of customer information occur at VG Trading Company.

Table 2: Business Impact Analysis Focusing on Specific Costs Following a Cyber-Attack

Above The Surface Impact	Impact Analysis
Customer breach notifications	The process requires at least six months and, at an expense of $0.5 million, this figure represents 0.6% of the total cost of a breach
Customer protection at the post-breach stage	This process is projected to take three years and attract a cost of $1.05 million, accounting for 1.25% of the breach's total cost
Regulatory compliance	This step is likely to take two years and attract a cost of $0.2 million, accounting for 0.12% of the cost of the breach
Crisis or public relations communication	Perceived to last five years, the procedure is likely to attract a cost of $0.05 million, reflecting 0.06% of the entire cost of the breach
Attorney fees and legislation	Taking about five years, the procedure could attract $0.5 million, translating into 0.6% of the breach's total cost
Cyber security improvements	The first year (following the leakage of customer data) is likely to require $0.7 million, representing 0.83% of the total cost
Technical investigation	The need for such investigations, if conducted effectively, could last six weeks and cost $0.05 million, an equivalent of $0.05 million, an equivalent of 0.06% of the total cost of the breach
Below The Surface Impact	**Impact Analysis**
Insurance premium costs	Stretching to three and more years, these costs are likely to be about $2 million and account for 2.38% of the total cost of the breach (over three years)
Operational cost towards raising debt	At around $3 million, these expenses lie at 3.57% of the total cost arising from the breach
Operational disruption	Emerging as the worst hit operation in case of a customer data breach at VG Trading Company, the disruption might prompt $1.5 million and reflect 1.79% of the total
Lost value of customer relationships	This area is likely to prompt significant and a combination of short-term and long-term investment to restore company reputation and operations at VG Trading Company. As such, the approximate cost lies at $21.5 million of the total (over three years), representing 25.61% of the total
Value of lost contact revenue	In most cases, it has been documented that a customer data breach makes this hidden cost to lie at around 49.43% over three years (Abomhara & Koien 2015)
Devaluation of trade name	On a five-year period, such breaches have been found to cause these losses and account for about 13.7% of the total (Amoroso 2013)
Loss of intellectual property	Most of the existing recommendations fail to affix values to this risk but its likelihood of emerging due to cyber security events such as customer data breaches cannot be overemphasized

III. Conclusion and Recommendations

From the above business impact analysis, it is evident that the "below the surface costs" of the breach outperform the "surface costs" accruing from a cyber security event such as that which involves the leakage of sensitive customer data. From the qualitative perspective, the two dominant issues likely to accrue include the loss of customers and the loss of reputation at VG Trading Company. To mitigate these risks, VG Trading Company needs to implement a number of controls. Some of these controls include:

- The maintenance of accurate inventories of control system devices and the elimination of their exposure to external networks
- The application of firewalls and the implementation of network segmentation
- The use of secure remote access networks (such as Virtual Private Network – VPN)
- The implementation of system logging and the establishment of role-based access controls
- The use of strong passwords
- The implementation of necessary updates and patches
- Implementation of employee cyber security training programs
- Implementation of measures to detect compromises, including intrusion detection systems (IDSs)

References

[1] Abomhara, M., & Koien, G.M. (2015). Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks. *Journal of Cyber Security*, 4, 65-88.

[2] Walker, C., & Conway, M. (2015). Online terrorism and online laws. *Dynamics of Asymmetric Conflict*, 8(2), 156-175.

10.9756/SIJCSEA/V7I4/03010020403
ISSN: 2321-2381